DETAILED ACTION

1. The Office Action is responsive to the communication filed on 08/06/2009.

2. Claims 1-12, 15-17, 19-31, 34-36, 38, and 41 are pending in the application.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 1-4, 8-9, 12, 15-17, 19-23, 27-31, 34-36, 38-39, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clifton et al. (Developing Custom Intrusion Detection Filters Using Data Mining, IEEE, 2000) in view over Cuppens (Managing Alerts in Multi-Intrusion Detection Environment, IEEE, 2001) and in view over Denning (An Intrusion Detection Model, IEEE, 1987), in view over Vikaykumar (USPN 5745896), and in view over Kay (USPN 20040099125), and in further view over Julisch (Mining alarm clusters to improve alarm handling efficiency, IEEE, 2001)

6. As per claim 1, Clifton et al. teaches a method for investigating messages passed in a message-passing environment, the method comprising:

collecting message traces ([Sequential Data Mining], [Figure 2] e.g., Log (Event, FromIP, ToIP, time), i.e., message trace. A message trace is interpreted as a message generated by a machine comprising time information. The message trace further identifies the source of the message) from at least one participant (e.g., machines on a network) in the message-passing environment (e.g., network), wherein each message trace is a series of messages originating from or sent to the at least one participant ([Figure 2] e.g., it is interpreted that an attacker is represented via a machine. A machine may generate multiple attacks. The attacks are identified via Log (Event, FromIP, ToIP, time). The attacks from one machine or machines represents a series or more than a single attack. As applied to a relational database, discussed below, messages may be grouped together within the relational database forming a group or sequence), ordered by time (e.g. basic schema includes time where samples are generated over a two week period and stored in a relational database), wherein each message has a first piece describing transfer of information (e.g., Log (FromIP, ToIP)) and a second piece describing an operation being performed in the message (Log(Event));

converting identifying information ([Sequential Association Mining] e.g., basic scheme, i.e., log data, identifies machine information) pertaining to the at least one participant (e.g. machine) into an indication of a role played (e.g., attacker. A role also pertains to an intrusion attempt) by the at least one participant in the message- passing environment (e.g. network);

assembling the messages into at least one message sequence ([SEQUENTIAL ASSOCIATION MINING], [Preliminary Results] e.g., we analyzed these logs for 2-, 3-, 4-, and

5-event sequences. A message sequence is interpreted as a grouping of messages. In one case, 2, 3, and 4-events are grouped. In another case, a relational database (discussed below) is used to store log data group together messages from a source. For example, if 20 messages are sent from sourceIP, then a relational database would be able to group these together. A message sequence (e.g., grouping) is taught in this case by grouping together 2, 3, 4, and 5-events),

wherein assembling the message sequences comprise combining multiple message traces (e.g., log(event, fromIP, toIP, time) into the at least one message sequence (e.g., 2,3,4, and 5-events), each message trace pertaining to one or more messages transmitted by, or received at, a participant (e.g., it is understood that a machine generates an attack, identified as an alarm. Log(event, FromIP, ToIP) is a message received, transmitted at a machine) , wherein the combining multiple message traces is based on:

a specified participant (FromIP, ToIP),

a specified time frame (e.g., one-minute window),

a transaction nature ([Straightforward Count] e.g. Syn Flood, ident, print), and

the role played by the specified participant (e.g., FTP user) ([Figure 2], [Preliminary Results]);

analyzing the at least one message sequence ([Number of Occurences]) from the message-passing environment (e.g., machine based network) to extract information (e.g., count) regarding the at least one participant (e.g.. machine) in the message-passing environment

However, Clifton et al. does not teach a reference message sequence. Denning teaches a reference sequence ([VII. C. Anomaly-Record Rules] e.g., comparing observations to known patterns of events, i.e., reference sequence. It is interpreted that a pattern is a sequence of events used to identify an abnormal or normal sequence of events. For example, two consecutive events

include failed password attempts. This corresponds to a 2-event, as applied to Clifton. By comparing 2,3, and 4-events with predetermined patterns of normal 2,3,-4 events, an abnormal condition can be brought to the attention of security.)

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to provide for a means to identify a normal set of events and an abnormal set of events. Clifton et al. teaches that 2,3, and 4-events that may corresponding to logged data. The events include a first command followed by a second command (e.g., 2-event). As applied to Denning, the 2-event would be observed and compared to a reference pattern (e.g., sequence) of normal/abnormal events. It is desirable to know whether a 2,3, and 4-event corresponds to an anomaly, and it would have been obvious to compare a series of events (e.g. message sequences) with a reference sequence of events (e.g., pattern of events) to ascertain event sequence anomalies. (For example, Clifton would teach a 2-event (e.g., password fail 1, password failed 2). By comparing this 2-event with a normal pattern (e.g., password fail, password successful), the first 2-event (e.g., message sequence) could be identified as abnormal)

Clifton et al., as modified, teaches a data matrix ([Sequential Association Mining] e.g., relational database where query functions are readily employed to sort, categorize, and group data within the database using keys) based on information in the at least one message sequence (Log(Event, FromIP, ToIP, time. *It is interpreted that a relational database would also enable one of ordinary skill in the art to view all messages from a single source, receiver, or event. From example, if a source sent twenty messages, all messages from that source could be grouped together using a query. In effect, this also functions as a message sequence (e.g., grouping)

However, Clifton et al. but does not teach cluster analysis is applied to the at least one message sequence. Cuppens teaches performing cluster analysis to identify and cluster alerts from data in its relational database ([4. Alert Clustering, 4.1 Similarity Relation) and forming at least one cluster based on the data matrix (e.g., relational database) ([Alert Clustering |4.1-4.2.3])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to group together similar event types (2, 3, and 4-events) to visually illustrate similar and dissimilar grouping of events. All prior art pertains to the same field of endeavor (e.g., intrusion detection), and it would have been obvious to apply clustering techniques to a data-set as an efficient and optimal means of analyzing data.

However, Clifton et al., as modified, does not teach forming at least one cluster based on the data matrix where the <u>at least one cluster includes the reference sequence</u> (e.g., the claim language is interpreted as forming individual clusters for each sequence. The claim language does not state one cluster comprises <u>both</u> a reference sequence and other types of message sequences, as per applicant's specification).

Clifton et al. teaches multiple message sequences ([Sequential Association Mining]), Denning teaches a reference message sequence ([VII. C. Anomaly-Record Rules] e.g., comparing observations to known patterns of events, i.e., reference sequence) Cuppens teaches clustering groups of related messages ([Section 4, Alert Clustering])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to cluster individual sequences as to form separate clusters. The motivation is to provide clusters for individual message sequences and reference messages sequences as a means to compare groups of normal observations to groups of anomalous observations. As applied to

the prior art, individual clusters are developed, wherein each cluster comprises a number of message sequences.

However, Clifton et al. does not teach that the aforementioned clusters are sorted into a ranked order based on a number of members associated with each cluster, the sorting prioritized from least members to most members associated with each of the at least two clusters. Kay teaches solving the pertinent problem of sorting a group from lowest to highest as a function of the number of items in a set ([0254])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to applying a sorting means to a group of clusters, as taught by Cuppens. Since new or emerging message sequences that occur infrequently (e.g., fewer in number) may pose a significant threat and/or require specific analysis opposed to frequent and well known sequence types (e.g., occurring in higher numbers), it would have been obvious to bring the aforementioned sequences to light via sorting clusters from lowest to highest, as to take into account and place emphasis on potentially new or isolated instances of potentially harmful sequences.

outputting the information (e.g., information is interpreted as any information pertaining to a participant. Here, information would be participant activity or message context. See Cuppens, [Figure 2], [Section 5 - Merging Alerts and Conflict Resolution] e.g., applying cluster results,)

However, Cuppens does not teach creating a table format based on the sorting into a ranked order, each cluster represented in the table format is linked to information regarding an associated message sequence. Julisch teaches a table comprising multiple alarm clusters ([Table 1]) , where it would be obvious to list the cluster alarms in ascending order based on the number

of items in the Cluster (e.g., supra Kay discussion), where the information in Table 1 is linked to information (e.g., attack type of participant. For example, when participant messages have a URL containing "%2E) regarding a message participant.

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to list the types of clusters in a table format, where each cluster is listed in ascending order (e.g., matter of design choice to list elements in ascending order) Each cluster in the table is linked to information (e.g., context fields, attack type, src-IP information, etc) gathered from each participant

[**Examiner note:** The claim analysis is structured to show that log data is stored in a relational database. A relational database, i.e., data matrix, enables the log data to be sorted and grouped together. The groups, whether 2-, 3-, 4-, or 5-events may be generated from the relational database using the logic used to generate the 2,3,4, and 5-event sequences. Additionally, messages from a sender and receiver may be grouped within the relational database to show all messages from the source/destination. This would represent a group or message sequence from a single participant. A similarity measure, as taught by Cuppens, shows how any grouping may be compared for the purpose of clustering. The principles of a relational database (e.g., references cites) illustrate the use of primary keys, sorting, grouping, and count functions as a way to mine data. <u>See Vijaykumar (USPN 5745896) for applications of queries, grouping, counting, and other intended functions provided with a relational database</u>)

7. As per claims 2 and 21, Clifton et al. teaches the method according to claim 1, wherein the message- passing environment is a network environment including plural participants coupled together via a network ([ABSTRACT])

8. As per claims 3 and 22, Clifton et al. teaches the method according to claim 2, wherein the network uses an Internet Protocol to transmit messages between participants ([Preliminary Results] e.g., FTP)

9. As per claims 4 and 23, Clifton et al. teaches the method according to claim 2, wherein the messages express the information in one of a plurality of message formats ([Preliminary Results] e.g., SYN Flood, ident, print, FTP (e.g., different formats)

10. As per claims 8 and 27, Cuppens teaches the method according to claim 1, wherein the message passing environment is a machine or system (e.g., alert based management system) including plural interacting components that function as message participants (e.. IDS modules) that function as message participants ([Figure 1] e.g., a client communicating with a central system would also include a software module (e.g., O/S, interface modules) for communicating over the network. The claim is interpreted as a network comprising a central system in communication with distributed clients, where a central system has software to collect and analyze network traffic)

11. As per claims 9 and 28, Cuppen teaches the method according to claim 1, wherein the message passing environment is a software program (e.g. alert based management system) including plural interacting software modules (e.g., IDS) that function as message participants ([Introduction], [Figure 1])

12. As per claim 12, Clifton et al. teaches the method according to claim 1, wherein the assembling comprises assembling plural message sequences (e.g., event logs are assembled into 2, 3, and 4-events), and analyzing comprises analyzing the plural message sequences (e.g., as modified, clustering is performed, supra claim 1 for pertinent citations and discussion)

13. As per claim 15, Clifton et al., as modified teaches the method according to claim 1, wherein the forming of the data matrix (e.g., relational database, supra Cuppens) involves extracting features ([Preliminary Results] e.g., Event, FromIP, ToIP) from said at least one message sequence (e.g. based on the grouping of similar messages from ToIP, a relational database counts the number of occurences), including extracting numerical counts (e.g., Count) for at least one feature present in the message sequence (e.g., counting number of messages sent from FromIP, for example), the feature including at least one of: a message command type, a sender/receiver pair (Log(FromIP, ToIP), a property of the message and an application-level property (It is interpreted that a relational database may receive event log and group (FromIP, ToIP, and Events) such that events from a sender may be classified together, events from a receiver may be classified, and the number of events may be sorted to include 2, 3,4, and 5-events)

14. As per claim 16, Cuppens teaches the method according to claim 1, wherein the forming of the data matrix involves forming a similarity measure ([Section 4. Alert Clustering] e.g., similarity function) which measures the difference between said at least one message sequence and another message sequence (e.g., when a new alert is generated, the function determines the existent of alerts in a database that can be linked. A similarity relation is defined between two alert messages. As applied to a relational database, groups of messages within the database may be compared via applying the similarity function), wherein forming a similarity measure includes at least one of: string/sequence matching (e.g., similarity relation links Entity 1 and Entity 2) and comparing said at least one message sequence with an optimal functioning sequence, a good

server trace, a bad server trace, and a known sequence from an alternate message-passing environment.

15. As per claim 17, Cuppens teaches the method according to claim 1, wherein the analyzing involves identifying results of the cluster analysis ([4.2.1- 5], [6.2] e.g., providing result to correlation function for further analysis) that may warrant further investigation, wherein the identifying includes comparing the at least one message sequence against a formal model of the message passing environment and placing the at least one message sequence into one or more clusters representing adherence to the formal model, non-adherence to the formal model and "interesting", wherein "interesting" includes indicia of beneficial phenomena, anomalous conditions, and other features which cause the at least one message sequence to be singled out from other message sequences ([4.2, 4.2.2, 4.2.3] e.g., 'at least one' of specified either selecting a) comparing a sequence against a formal model or b) interesting includes other features. Here, clustering may occur using time, source/target similarity, and classification similarity (e.g., interesting)

16. As per claims 19 and 38, Clifton et al., as modified, teaches a computer readable medium (e.g., intrusion detection system) including machine readable instructions for implementing the collecting, assembling, analyzing, and outputting recited in claim 1 (e.g. instructions, i.e., code, is implemented in Cuppens | Denning to provide pattern matching, data logging. The relational database implements code to sort data. Cluster analysis implements code to group data based on similarity measures.

17. Claim 20 is rejected under over Clifton et al. (Developing Custom Intrusion Detection Filters Using Data Mining, IEEE, 2000) in view over Cuppens (Managing Alerts in Multi-

Intrusion Detection Environment, IEEE, 2001) and in further view over Denning (An Intrusion Detection Model, IEEE, 1987), and in view over Vikaykumar (USPN 5745896), and in view over Kay (USPN 20040099125), and in further view over Julisch (Mining alarm clusters to improve alarm handling efficiency, IEEE, 2001), and in further view over Hofmeyr et al., (Intrusion Detection using Sequences of System Calls, 1998), and in further view over Na et al. (USPN 20030149679)

18. As per claim 20, Clifton et al., as modified, teaches an apparatus for investigating messages passed in a message-passing environment, the apparatus comprising:

message aggregation logic configured to collect a plurality of messages from at least one participant in the message-passing environment ([Sequential Associations] e.g., Log(Event, FromIp, ToIP), i.e., aggregation logic) As modified by Cuppens, a relational database is used to store the data), and to assemble the messages into at least one message sequence (e.g., 2, 3,4, and 5-events and/or using a relational database to group/sort data using attributes (From, To, Event), wherein teach message has a first piece describing transfer information (e.g., From IP, ToIP) and a second piece describing an operation being performed in the message (e.g. event), wherein assembling the messages into at least one message sequence us based on:

a specified participant (FromIP, ToIP),

a specified time frame (e.g., one-minute window),

a transaction nature ([Straightforward Count] e.g. Syn Flood, ident, print), and

the role played by the specified one participant (e.g., FTP user) ([Figure 2], [Preliminary Results] e.g, it is obvious that given a To of FromIP, a specific participant may be identified via any search query or alogorithm);

analysis logic configured ([Preliminary Results] e.g., Counts) to analyze said at least one message sequence from the message passing environment to extract information regarding at least the one participant in the message-passing environment (e.g., number of 2-event counts), wherein the analysis logic (e.g., supra claim 1, Dennings, VII.C e.g. pattern matching) is further configured to compare said at least one message sequence with a reference message sequence, the reference message sequence comprising a sequence that reflects an error-free operation in the message passing environment (e.g., supra claim 1 discussion)

cluster analysis logic (e.g., Section 4, Alert Clustering, supra Cuppens discussion, claim 1) configured to perform cluster analysis to group the at least one message sequence and the reference message sequence into at least one cluster (e.g., supra claim 1 discussion where separate clusters, i.e., at least one cluster, are formed per sequence type), wherein the cluster analysis logic is configured to form a data matrix based on information in the at least one message sequence and form the at least one cluster based on the data matrix (e.g., supra claim 1 discussion); and

However, Clifton et al., as modified, does not teach the cluster analysis logic is configured to measure a distance between two or more message sequences of each cluster formed by the cluster analysis logic. Cuppens teaches grouping similar sequences together in the form of a cluster. Hofmeyr teaches performing a similarity measure (e.g., Hamming distance) between two message sequences ([Section 3.2])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to perform Hamming distances across multiple message sequences as to enable similar messages to be grouped for the purpose of cluster analysis.

Output logic (see Cuppens, Section 4) but does not teach outputting the information as a two-dimensional presentation of the at least one cluster and indicating the reference sequence and the distance associated with the at least one message sequence. Na teaches outputting the information (e.g., clusters are formed based on grouping similar message sequences.) in the form of a two dimensional representation ([Figure 2], [0038]). Clifton et al., as modified, teaches that multiple clusters are formed by grouping similar message sequences together, based on the teachings of Julisch, supra claim 1 discussion). Denning teaches a reference sequence ([VII. C. Anomaly-Record Rules] e.g., comparing observations to known patterns of events, i.e., reference sequence. As modified, a normal sequence is clustered separately from the other sequence types for the purpose of comparison, supra claim 1). Since clusters are formed via using the teachings of Hofmeyr (e.g., Hamming distance), it is obvious that the clusters, once formed, indicate the distance or similarity of message groups. One of ordinary skill in the art would in effect represent similar groups via a cluster, identify reference sequence cluster from attack type clusters for comparison, and knowing that distance (e.g., whether Hamming or Euclidean) metrics were used to form the cluster, such a cluster is an indication of the relative distances between each message sequence

19. As per claim 29, Clifton et al., as modified teaches the apparatus according to claim 20, wherein the message aggregation logic is further configures to convert identifying information pertaining to said at least one participant (e.g., FromIP, ToIP, Ftp User) into an indication of a role played by the participant in the message passing environment (e.g., role is not defined. A role may be an intrusion attempt, an attacker, recognizing an FTP user, etc)

20. As per claim 30, Clifton et al. as modified, teaches the apparatus according to claim 20, wherein the message aggregation logic is further configured to combine multiple message traces into said at least one message sequence (e.g., 2,3,4,5-events and/or grouping similar FromIP using a relational database), each message trace pertaining to one or more messages transmitted by and/or received at a participant (e.g., Log(Event, From, To, time)

21. As per claim 31, Clifton et al. teaches the apparatus according to claim 20, wherein the message aggregation logic is further configured to assemble plural message sequences (e.g., group together in the table, Preliminary Results), and the analysis logic is further configured to analyze the plural message sequences (e.g., Counts)

22. As per claim 34, Clifton, as modified, teaches the apparatus according to claim 20, wherein the analysis logic is configured to form the data matrix (e.g., relational database) by extracting features (e.g., (FromIP, ToIP, and/or Event) from said at least one message sequence (e.g., when a relational database is used, messages may be grouped together from the same participant, i.e., FromIP. Once grouped, messaged may be counted and/or compared to other groups from other participants)

23. As per claim 35, Clifton et al., as modified, teaches the apparatus according to claim 20, wherein the analysis logic is configured to form the data matrix by forming a similarity measure which measures the difference between said at least one message sequence and another message sequence (e.g., supra claim 16)

24. As per claim 36, Clifton et al., as modified, teaches the apparatus according to claim 20, wherein the analysis logic is further configured to identify results of the cluster analysis that may warrant further investigation (e.g., supra claim 17)

25. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clifton et al. (Developing Custom Intrusion Detection Filters Using Data Mining, IEEE, 2000) in view over Cuppens (Managing Alerts in Multi-Intrusion Detection Environment, IEEE, 2001) and in further view over Denning (An Intrusion Detection Model, IEEE, 1987), and in further view over Vikaykumar (USPN 5745896).

26. As per claim 39, Clifton et al. teaches a method for investigating messages passed in a message-passing environment, the method comprising:

means for collecting message traces ([Sequential Data Mining], [Figure 2] e.g., Log (Event, FromIP, ToIP, time), i.e., message trace. The means for claim terminology is interpreted as software. It is interpreted that software is used to collect the messages (e.g., Log (Event, FromIP, ToIP, and time). A message trace is interpreted as a message generated by a machine comprising time information. The message trace further identifies the source of the message) from at least one participant (e.g., machines on a network) in the message-passing environment (e.g., network), wherein each message trace is a series of messages originating from or sent to the at least one participant ([Figure 2] e.g., it is interpreted that an attacker is represented via a machine. A machine may generate multiple attacks. The attacks are identified via Log (Event, FromIP, ToIP, time). The attacks from one machine or machines represents a series or more than a single attack. As applied to a relational database, discussed below, messages may be grouped together within the relational database forming a group or sequence), ordered by time (e.g. basic schema includes time where samples are generated over a two week period and stored in a relational database), wherein each message has a first piece describing transfer of information (e.g., Log (FromIP, ToIP)) and a second piece describing an operation being

performed in the message (Log(Event));

a means for converting identifying information ([Sequential Association Mining] e.g., basic scheme, i.e., log data, identifies machine information. Software is interpreted as the 'means for' because all references utilized implement code for the collecting and data analysis) pertaining to the at least one participant (e.g. machine) into an indication of a role played (e.g., attacker. A role also pertains to an intrusion attempt) by the at least one participant in the message- passing environment (e.g. network);

means for assembling the messages into at least one message sequence ([SEQUENTIAL ASSOCIATION MINING], [Preliminary Results] e.g., software is interpreted as the 'means for'. we analyzed these logs for 2-, 3-, 4-, and 5-event sequences. A message sequence is interpreted as a grouping of messages. In one case, 2, 3, and 4-events are grouped. In another case, a relational database (discussed below) is used to store log data group together messages from a source. For example, if 20 messages are sent from sourceIP, then a relational database would be able to group these together. A message sequence (e.g., grouping) is taught in this case by grouping together 2, 3, 4, and 5-events),

wherein assembling the message sequence comprises combining multiple message traces (e.g., log(event, fromIP, toIP, time) into the at least one message sequence (e.g., 2,3,4, and 5-events), each message trace pertaining to one or more messages transmitted by, or received at, a participant (e.g., it is understood that a machine generates an attack, identified as an alarm. Log(event, FromIP, ToIP) is a message received, transmitted at a machine) , wherein the combining multiple message traces is based:

a specified participant (FromIP, ToIP),

a specified time frame (e.g., one-minute window),

a transaction nature ([Straightforward Count] e.g. Syn Flood, ident, print), and

the role played by the specified participant (e.g., FTP user) ([Figure 2], [Preliminary Results]);

means for analyzing the at least one message sequence ([Number of Occurences]) from the message- passing environment (e.g., machine based network) to extract information (e.g., count) regarding the at least one participant (e.g.. machine) in the message-passing environment. (the means for language is interpreted as software means. Here, clustering utilizes software code to access a relational database and subsequently perform clustering)

However, Clifton et al. does not teach a reference message sequence. Denning teaches a reference sequence ([VII. C. Anomaly-Record Rules] e.g., comparing observations to known patterns of events, i.e., reference sequence. It is interpreted that a pattern is a sequence of events used to identify an abnormal or normal sequence of events. For example, two consecutive events include failed password attempts. This corresponds to a 2-event, as applied to Clifton. By comparing 2,3, and 4-events with predetermined patterns of normal 2,3,-4 events, an abnormal condition can be brought to the attention of secuirty.)

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to provide for a means to identify a normal set of events and an abnormal set of events. Clifton et al. teaches that 2,3, and 4-events that may corresponding to logged data. The events include a first command followed by a second command (e.g., 2-event). As applied to Denning, the 2-event would be observed and compared to a reference pattern (e.g., sequence) of normal/abnormal events. It is desirable to know whether a 2,3, and 4-event corresponds to an

anomaly, and it would have been obvious to compare a series of events (e.g. message sequences) with a reference sequence of events (e.g., pattern of events) to ascertain event sequence anomalies. (For example, Clifton would teach a 2-event (e.g., password fail 1, password failed 2). By comparing this 2-event with a normal pattern (e.g., password fail, password successful), the first 2-event (e.g., message sequence) could be identified as abnormal)

Clifton et al., as modified, teaches a data matrix ([Sequential Association Mining] e.g., relational database) based on information in the at least one message sequence (Log(Event, FromIP, ToIP, time. *It is interpreted that a relational database would also enable one of ordinary skill in the art to view all messages from a single source, receiver, or event. From example, if a source sent twenty messages, all messages from that source could be grouped together. In effect, this also functions as a message sequence (e.g., grouping) but does not teach cluster analysis applied to the at least one message sequence. Cuppens teaches performing cluster analysis to identify and cluster alerts from data in its relational database ([4. Alert Clustering, 4.1 Similarity Relation) and forming at least one cluster based on the data matrix (e.g., relational database) ([Alert Clustering |4.1-4.2.3])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to group together similar event types (2, 3, and 4-events) to visually illustrate similar and dissimilar grouping of events. All prior art pertains to the same field of endeavor (e.g., intrusion detection), and it would have been obvious to apply clustering techniques to a data-set as an efficient and optimal means of analyzing data.

However, Clifton et al., as modified does not teach performing cluster analysis to group at least one message sequence and the reference message sequence. Cuppens teaches performing

cluster analysis. Clifton teaches multiple types of message sequences. Denning teaches a reference sequence ([VII. C. Anomaly-Record Rules] e.g., comparing observations to known patterns of events, i.e., reference sequence.

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to provide separate clusters for each type of message sequence. The motivation is to group similar sequences for the purpose of comparison. (Applicant's claim terminology does not claim one cluster comprising both types of sequences)

means for storing the at least one message sequence in a master collection of message sequences (e.g., relational database, supra Cuppens Introduction. A relational database stores any message grouping)

means for culling the master collection of message sequences for at least one subset of a message sequence based on specified criteria including one of more of: a specified time range, transaction type, participants involved in at least one message exchange, objectives of an analyst and a nature of the messaqe- passing environment involved (e.g., a relational database enables data to be sorted via time, which in view over Clifton, i.e., time analysis, enables a certain sub-subset of messages to be localized. The From and To participants may be grouped according to time, similar events, etc using a relational database, etc); and

means for storing the at least one subset for subsequent analysis (e.g., relational database, i.e., means for storing);

means for outputting the information ([Figure 2], [Section 5 - Merging Alerts and Conflict Resolution] e.g., applying cluster results. Software is interpreted as the means)

27. As per claim 41, Clifton et al., as modified, teaches the apparatus according to claim 20, wherein the reference message sequence is a sequence that reflects known failure conditions within the message passing environment (e.g., supra claim 1 discussion)

28. Claims 5-7 & 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clifton et al. (Developing Custom Intrusion Detection Filters Using Data Mining, IEEE, 2000) in view over Cuppens (Managing Alerts in Multi-Intrusion Detection Environment, IEEE, 2001) and in further view over Denning (An Intrusion Detection Model, IEEE, 1987), and in further view over Greifeneder et al. (USPN 20040243349)

29. As per claims 5 and 24, Clifton et al., as modified, teaches a analyzing network traffic for events but does not teach where the messages include information expressed in a markup language. Greifeneder et al teaches that network traffic may comprise documents including XML, GIF, and JPG communicated using network protocols, including but not limited to SOAP ([0064], [0019])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Clifton et al. to include xml based messages. Scarfe et al. teaches collecting information pertaining to network traffic for classification and analysis. Greifeneder et al. teaches a method and system for monitoring and the analysis of networked systems. Xml based messages are a common format utilized in network communication. Since xml messages include data about data, it would have been obvious to group and analyze such messages for pertinent information about the behavior of a sender/receiver within a network.

34. As per claims 6 and 25, Greifeneder et al. teaches wherein the markup language is xml ([0064] e.g. XML)

35. As per claims 7 and 26, Greifeneder et al. teaches wherein the network uses Simple Object Access Protocol to transmit messages between participants ([0019] e.g. SOAP)

Response to Amendment

36. The amendment, filed 08/06/2009, has been entered.

Response to Arguments

37. Applicant's arguments filed 08/06/2009, have been fully considered but they are not persuasive. Applicant's amendment to the claim language has based a collection of message traces on a specified participant, a specified time frame, a transaction nature, and the role played by at least the specified participant. Each reference teaches the above elements, which taken in combination applying KSR, provides important identifying information from which to identify an abnormal sequence of messages. When given the identity of a participant, i.e., To and From IP, the time range from which to sample the messages, the transaction nature (e.g., type of attack, repeated requests for information, etc), and the role play by the specific participant (e.g., one role would be the requester, i.e., ToIP while another role could be classified as an attacker. A skilled artisan has motivation to combine contextual information to provide an indicia of who is sending a message, what is this message and how many occurred in a time frame, the type of message, and a role, i.e., given the transaction nature of a message one may deduce the role being played by the sender. For example, a flood attack, sending a virus, sending a simple request, etc all provide a transaction nature from which the role of the entity sending this information is identified. For example, ToIP indicates a role of sender.

Conclusion

38. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARRIN DUNN whose telephone number is (571)270-1645. The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DD/
03/24/10

/Albert DeCady/
Supervisory Patent Examiner
Art Unit 2121